



This essay is published on Panorama Portal at 01/09/2022.

Bu analiz Panorama Portalı'nda 01/09/2022 tarihinde yayınlanmıştır.

[10.13140/RG.2.2.29794.81600/1](https://doi.org/10.13140/RG.2.2.29794.81600/1)

E-ISSN: 2718-0549

Bu yazıya atıf için: Sıtkı Egeli, "Rusya-Ukrayna Savaşı'nda Kullanılan Yeni ve Bozucu Teknolojiler" ,*Panorama*, Çevrimiçi Yayın, 01 Eylül 2022, <https://www.uikpanorama.com/blog/2022/09/01/uk-ru/>

Rusya-Ukrayna Savaşı'nda Kullanılan Yeni ve Bozucu Teknolojiler

Rusya Federasyonu'nun Ukrayna topraklarını işgal etmek ve Ukrayna'nın egemen bir devlet olarak varlığına son vermek amacıyla 24 Şubat 2022'de başlattığı savaşın siyasi, ekonomik, jeopolitik, stratejik, taktiksel ve operasyonel boyutları yoğun şekilde tartışıldı ve tartışılmaya da devam ediyor. Bu yazıda, hakkında bazı yüzeysel haberlere ve yorumlara rastlanmakla birlikte, Rusya-Ukrayna Savaşı'nın Türk kamuoyu ve akademik çevrelerce pek irdelenmeyen bir veçhesine odaklanarak, çatışmaların başlamasından bu yana taraflarca kullanılan “Yeni ve Bozucu Teknolojiler”i (YBT) ele alarak, bunların etkinliği ve kısa-orta vadeli yansımalarını inceleyeceğiz.

Öncelikle, son yıllarda uluslararası güvenlik çalışmalarının hemen her sahasında kendine giderek artan şekilde yer bulan YBT kavramının tanımlanmasını ve içeriğinin belirlenmesi yerinde olacaktır. YBT kavramındaki “yeni” olgusu, son dönemde süratli gelişmelerin kaydedildiği ve/veya yakın gelecekte kritik ve çığır açıcı yeni gelişmelerin beklendiği teknoloji alanlarına işaret etmektedir. “Bozucu” ifadesinden anlaşılması gereken ise, devletler arasındaki caydırıcılık denklemleri, silahlar ile silahlanmanın kontrolüne yönelik düzenlemeler ya da tırmanma ve kriz yönetimi konularında aşındırıcı etkiler yaratarak, uluslararası dengeleri ve istikrarı olumsuz yönde etkileyebilecek [teknolojik gelişmelere](#) atıf yapmaktadır.

Dolayısıyla YBT denildiğinde, gerçekten yeni olan ve mevcut dengeler üzerinde bozucu etkiler yaratabilecek teknolojilerden istifade eden silahlar ve saldırı imkanları ile bunları destekleyen sistemler ve alt sistemler anlaşılmalıdır. Bir örnek vermek gerekirse, 2000’li yıllardan itibaren ABD’nin kayda değer yatırım yaptığı füze savunması, Rusya ve Çin tarafından kendi stratejik nükleer silahlarına yönelik bir tehdit olarak algılanmış ve bu algı bir yandan yeni stratejik silah türlerine yönelimi ve dolayısıyla başat güçler arasındaki silahlanma yarışını tetiklerken, diğer yandan da Anti-Balistik Füze (ABM) ve Orta Menzilli Nükleer Silahlar (INF) gibi silahların kontrolüne yönelik köşe taşı niteliğindeki anlaşmaların sonunu getirmiştir. Bu itibarla, füze savunması [birçok gözlemci](#) tarafından YBT olarak [görülmemektedir](#).

YBT’nin tanımı nispeten açık ve kesin olduğu halde, hangi teknolojilerin, hangi silahların ve hangi yeteneklerin YBT kapsamına dahil edilmesi gerektiğine dair savunma ve savunma sanayii çevrelerinde, akademik camiada ve siyaset yapıcılar arasında fikir birliği yoktur. Zira, hangi teknolojilerin bu kriterleri karşıladığı sübjektif bazı çıkarım ve varsayımlara dayanmaktadır. İlâveten, incelenen her bir teknolojinin gelecekte alabileceği şeklin ve potansiyelinin önceden kestirilmesinde belirsizlikler olduğu gibi, yeni teknolojilerin birçoğunu çevreleyen gizlilik perdesi de kesin yargılara varılmasını ve geleceğe yönelik çıkarımlarda bulunulmasını güçleştirmektedir. Tablo-1’de, son dönemde gerek akademik çevreler gerekse NATO ve Avrupa Birliği gibi örgütlerce hazırlanan bazı rapor ve çalışmalara göre YBT niteliği taşıdığı iddia edilen teknolojiler listelenmiştir. Görüleceği üzere, YBT muamelesi görmeye aday teknolojiler büyük çeşitlilik gösterdiği gibi, bunların hangilerinin YBT olarak değerlendirilmesi gerektiği üzerinde de bir uzlaşma bulunmamaktadır.

Tablo-1: Muhtelif çalışmalara göre Yeni ve Bozucu Teknolojiler.

FAS Special Report	NATO STO Report	EUNPDC Paper	KCL Weapons of Mass Distortion
Hipersonik	Hipersonik	Hipersonik	Hipersonik
Siber tehditler		Ağ Operasyonları	
Yapay Zekâ & Büyük Veri Analizi	Yapay Zekâ	Yapay Zekâ & Otomasyon	Yapay zekâ destekli siber saldırılar
	Veri		
	Otonom sistemler		Robot kümeleri
	Uzay	Uzay ve Karşı-Uzay	Küçük uydular, RPO, uydusavar
Yüksek güçlü lazerler			Yönlendirilmiş enerji
Tepeden ısrarlı algılama			Yapay zekâ destekli algılama
			Deepfake
	Kuantum		
	Yeni malzemeler ve imalat		
	Biyoteknoloji ve insan iyileştirme		
		Füze savunması	

Bu tabloya şubat ayından bu yana devam eden Rusya-Ukrayna Savaşı açısından bakıldığında, son dönemde birçok örgüt ve araştırmacı tarafından YBT olarak nitelendirilen teknolojiler ve yeteneklerden üçünün Rusya veya Ukrayna tarafından sahaya sürüldüğü görülmektedir. Belki daha da önemlisi, bahse konu üç teknoloji veya kabiliyetin, iki devlet arasında vuku bulan büyük çaplı bir konvansiyonel çatışmada ilk kez olarak kullanılıyor olmasıdır. Söz konusu üç YBT; i) hipersonik silahlar, ii) siber saldırılar ve iii) karşı uzay olup, bunların her birinin Rusya-Ukrayna Savaşı bağlamındaki kullanım şekli, etkinliği ve bu kullanımın kısa-orta vadedeki olası yansımaları takip eden alt başlıklarda ele alınacaktır.

Hipersonik silahlar

Hipersonik silah terimi, ses hızının beş misli ve üzeri süratlerde yol alabilen füzeler için kullanılmakla birlikte, bu kategorideki füzelerin gerçek ayırt edici özelliği, isimlerini borçlu oldukları yüksek süratlerinden ziyade, uçuşları sırasında manevra yapabiliyor olmalarıdır. Yoksa İkinci Dünya Savaşı'ndan bu yana kullanılmakta olan balistik füzeler de ses hızının beş, on, hatta yirmi beş mislini bulan süratlere ulaşabilmektedir. Fakat balistik füzeler uçuşlarını önceden öngörülebilir parabol şeklindeki “balistik” bir uçuş hattı boyunca gerçekleştirdiklerinden, başka bir ifadeyle ateşlendikten sonra manevra yapamadıklarından,

hipersonik silah olarak nitelendirilmiyorlar. Benzer şekilde, tespit edilmeden hedeflerine ulaşabilmek için radarların görüş alanının altındaki alçak irtifaları tercih eden seyir füzeleri de ani manevra yapabildikleri halde, görece yavaş uçtuklarından hipersonik silah kategorisine dâhil edilmiyorlar. Bu itibarla hipersonik silahlar, balistik füzelerin yüksek sürat avantajı ile seyir füzelerinin manevra yaparak hava ve füze savunma önlemlerini atlatabilme avantajını birleştiren farklı bir füze kategorisi olarak [nitelenebilir](#).

Son 20 yılda ABD'nin füze savunma alanında kaydettiği teknolojik sıçramaların, kendi stratejik nükleer füzelerinin caydırıcılığı üzerindeki aşındırıcı etkisini telafi etmek isteyen Rusya Federasyonu, ABD'nin füze savunma sistemlerini etkisiz kılma potansiyeline sahip hipersonik silahlara en büyük ve en erken yatırım yapan devletlerin başında gelmektedir. Nitekim Rusya, bu alanda ABD ve Çin'i geride bırakarak son beş yılda üç ayrı sınıfta hipersonik füzeyi envanterine dahil eden ilk devlet olmuştur. Bunlar, kıtalararası balistik füzelerce taşınan nükleer başlıklı *Vanguard*, hipersonik bir seyir füzesi olan *Zirkon* ve İskender taktik balistik füzelerinin uçaktan fırlatılabilen bir türevi olan *Kinzhal*'dır. Rusya-Ukrayna Savaşı'nın başlamasından yaklaşık üç hafta sonra Mig-31K uçağından ateşlenerek Ukrayna'daki bir mühimmat deposunu hedef alan bir Kinzhal füzesi, hipersonik silahların harp tarihindeki ilk operasyonel kullanımı [olmuştur](#). Takip eden aylarda Rusya'nın Ukrayna'daki hedeflere bir düzineden fazla Kinzhal füzesi ateşlediği [rapor edilmiştir](#).

800 kilometrelik uçuş menziline sahip Kinzhal füzesi, kendini taşıyan uçağın ateşleme anına kadar kat edebileceği azami mesafe de hesaba katıldığında 2,000 kilometre [menzile sahiptir](#). Klasik hassas güdümlü mühimmata kıyasla [en önemli ayırt edici niteliği](#), hedefine çok kısa sürede ve çok yüksek süratle (Rus kaynaklarına göre ses hızının 10 misli, bağımsız kaynaklara göreyse 6 misli) ulaşması ve uçuşu boyunca sık sık irtifa ve yön değiştirerek hem hedefini son ana kadar belli etmemesi, hem de füze savunma sistemlerini atlatabilmesidir. Rusya-Ukrayna Savaşı'nda Kinzhal füzelerinin hedeflerine yüksek isabet hassasiyetiyle ulaştıkları, dolayısıyla üzerlerine düşen görevi başarıyla yerine getirdikleri kabul edilmekle birlikte, Rusya'nın füze savunma sistemlerine sahip olmayan Ukrayna karşısında, ayırt edici özelliği füze savunma sistemlerini atlatmak olan Kinzhal gibi hem çok pahalı hem de stoklarda sadece birkaç düzinesinin mevcut olduğuna inanılan bir silahı niçin tercih etmiş olabileceği sorusu [cevaplanmaya muhtaçtır](#).

Öne çıkan açıklamalardan ilki Rusya'nın bu savaşı, daha önce Suriye'de yaptığı gibi, yeni geliştirdiği silahlar için test sahası olarak kullandığıdır. İkinci açıklama, Rusya'nın normalde bu tür hedeflere karşı kullanması beklenen yüksek isabet hassasiyetine sahip modern seyir füzesi ve balistik füze stoklarını büyük oranda tükettiği ve NATO'ya karşı asgari stratejik stoklarını muhafaza edebilmek için bir yandan Soğuk Savaş döneminden kalma eski ve isabet hassasiyeti çok düşük seyir füzelerini kullanıma sürerken, diğer yandan da Kinzhal gibi değerli ama daha güvenilir silahlarını kullanmaya [mecbur kaldığıdır](#). Bununla bağlantılı olarak, ABD kaynaklarına göre yüzde 60'a varan oranlarda başarısız olduğu ve hedeflerini vurmadığı iddia edilen modern Rus seyir füzeleri yerine, kritik önemdeki hedeflere karşı daha güvenilir ve garantili bulunan Kinzhal füzelerinin tercih edildiği [düşünülebilir](#). Olası bir diğer açıklama ise, Rusya'nın envanterindeki en yeni ve ses getirecek silahları kullanıma sürerek, Ukrayna halkı üzerinde baskı oluşturmayı ve kendi halkına moral vermeyi hedeflediği ve/veya NATO'ya karşı yeni silah tiplerine, hatta nükleer silahlara başvurarak savaşı tırmandırmaktan çekinmeyeceği [mesajını vermeye çalışması olabilir](#).

Öte yandan, hipersonik silahların Rusya-Ukrayna Savaşı'nda ilk kez kullanılmasının, savaşın seyri ve şu ana kadarki sonuçları üzerinde hiçbir kayda değer etki yaratmadığı da burada belirtilmelidir. Dolayısıyla taktiksel, operasyonel ve stratejik açılardan ele alındığında, son yıllarda bir YBT olarak hipersonik silahlar etrafında şekillenen uyarılar ve kaygılar büyük

oranda boşa çıkmıştır. Bu durumun ortaya çıkmasında, Rusya-Ukrayna Savaşı'nın özel şartlarının etkili olduğu ve Ukrayna'nın zaten sahip olmadığı füze savunma kabiliyetinin alt edilmesi için hipersonik füzelere ihtiyaç duyulmadığı gerçeğinin altı çizilmelidir. Diğer taraftan, görece gelişmiş füze savunma yeteneklerine sahip ABD, İsrail ve Japonya gibi devletler ile envanterine hipersonik silahlar dahil edebilecek olası ülkeler arasındaki kriz ve çatışma senaryolarında, hipersonik silahların varlığının kayda değer, istikrarsızlaştırıcı ve tırmandırıcı rol oynayabileceği göz ardı edilmemelidir. Ayrıca bu kategorideki silahların son yıllarda sadece ABD, Rusya ve Çin gibi başat güçler değil, Fransa, Hindistan, Japonya, Avustralya, Kuzey Kore ve İran gibi diğer pek çok devlet tarafından da geliştiriliyor olması, gelecekteki hem stratejik hem de bölgesel çatışmalarda hipersonik silahlara sıklıkla başvurulabileceğine işaret etmektedir. Sonuç itibarıyla, Rusya-Ukrayna Savaşı sayesinde, hipersonik silahlar artık geleceğe yönelik fütüristik bir teknoloji ve kavramsal bir düşünce olmaktan çıkarak, modern savaş alanlarının elle tutulur askeri güç unsurlarına dönüşmüştür.

Siber saldırılar

Devletlerin ve devlet dışı oyuncuların siber ortamdaki muhtelif işlevleri yerine getirmekte ve veri depolamakta kullandıkları donanım, yazılım ve ağların etkinliğinin azaltılması, bunların işlev ve içeriklerine zarar verilmesi, kesintiye uğratılması, bunlara erişimin engellenmesi ve/veya veri içeriklerinin ele geçirilmesine yönelik siber ortamdaki saldırılar, 2000'li yıllardan bu yana uluslararası güvenlik gündeminin öncelikli konuları arasında yer almaktadır. 2007'deki Rusya-Estonya gerginliği, 2008 Rusya-Gürcistan Savaşı, 2010 yılında İran'ın uranyum zenginleştirme altyapısına yönelik Stuxnet saldırısı ve 2014'te Kırım'ın Rusya tarafından işgaline eşlik eden siber ortamdaki manipülasyon ve müdahaleler göz önüne alındığında, siber saldırıların aslında yeni bir olgu olmadığı, dolayısıyla artık YBT tanımına uymadığı bile iddia edilebilir. Buna karşılık, Rusya-Ukrayna Savaşı'nda her iki tarafça da başvuru siber saldırıların yoğunluğu ve ayrıca bu saldırıların iki devlet arasındaki konvansiyonel bir çatışmanın doğrudan uzantısı ve tamamlayıcısı olarak ilk kez sahaya sürülmüş olması önemli bir dönüm noktasına işaret etmekte, bu itibarla detaylı şekilde incelenmeyi hak etmektedir.

Bu kapsamda dikkat çeken hususlardan ilki, Rusya'nın Ukrayna'ya yönelik siber saldırılarının etkileri ve sonuçlarının bariz şekilde gözlemlenmemiş olması sebebiyle, Rusya'nın çok korkulan siber savaş potansiyelini Ukrayna'ya karşı kullanmaktan imtina ettiği izleniminin [oluşmuş olmasıdır](#). Halbuki, savaşın ilerleyen evrelerinde kamuoyuyla paylaşılan yeni bilgiler sayesinde artık kuşku duyulmayan gerçek, Rusya'nın sadece konvansiyonel askeri saldırısını başlattığı 24 Şubat'ta ve takip eden günlerde değil, 24 Şubat'ın birkaç gün öncesinden başlayarak bugüne kadar görülmemiş yoğunlukta [siber saldırı faaliyeti içerisine girdiği](#) ve [elindeki imkanları sonuna kadar kullanmayı denediğidir](#). Bu yönüyle, Rusya'nın siber saldırıları konvansiyonel askeri hareketinin hazırlayıcısı ve tamamlayıcısı olarak kullanmış olması, siber güvenlik uzmanlarının uzun süredir uyardıkları gelecekteki konvansiyonel savaşların siber saldırılarla başlayacağı [öngörüsüyle](#) örtüşmektedir. Buna karşılık, uluslararası güvenlik çevrelerinin uzun zamandır gündeminde bulunan siber felç veya '*Siber Pearl Harbor*' kehanetleri gerçekleşmemiştir. Rusya'nın bir savaş durumunda Batılı devletleri siber saldırılarla dize getirebileceği uyarıları boşa çıkmıştır. Zira Rusya'nın konvansiyonel askeri kuvvetlerinin sergilediği zayıf performansın bir benzerinin siber ortamda yaşandığı ve siber saldırılarının 2/3'ünün başarısızlıkla sonuçlandığı [anlaşılmaktadır](#). Başarılı olan 1/3 oranındaki siber saldırı ise harekât alanındaki gelişmelerle eşgüdüm içerisinde yürütülmemiş, siber boyutta yaratılan fırsatlar fiziki savaş alanında avantaja çevrilememiş, dolayısıyla Rusya'nın çekinilen siber harp performansı [ortalamanın altında kalmıştır](#).

Fakat Rusya'nın siber saldırılardan umduğu sonuçları alamamasında denklemin sadece Rusya ayağı değil, Ukrayna ve Batı ayağındaki değişikliklerin de önemli rol oynadığı unutulmamalıdır. Çünkü Ukrayna ile destekçisi Batılı ülkelerin Kırım'ın 2014'teki işgalinden bu yana geçen zamanı iyi değerlendirerek, Rusya'nın siber saldırı potansiyelini etkisiz kılacak tedbirleri almış oldukları anlaşılmaktadır. Bu kapsamda, siber saldırılar karşısında ülkesel direncin (*resilience*) tesis edilmesi sayesinde, Rus siber saldırılarının yarattığı açıklar ve kesintilerin neredeyse anında giderilebildiği görülmektedir. Örneğin savaşın başlamasından bir gün önce Rusya, *FoxBlade* zararlı yazılımıyla Ukrayna devlet kuruluşlarının internet ortamındaki verilerini silmeyi başardığı halde, gerekli yedeklemelerin yapılmış olması sayesinde kaybedilen veriler [süratle yerine konabilmiştir](#). Benzer şekilde, Ukrayna'nın haberleşme ve internet hizmetleri, Rus birliklerinin ortak sınırı geçtiği saatlerde bir dizi siber saldırıyla durma noktasına getirilmiş, fakat telafi edici önlemlerin derhal devreye sokulmasıyla süratle ayağa kaldırılmıştır. Bir diğer çarpıcı örnekte, Ukrayna ordusunun kullandığı KA-ASAT haberleşme uydusuna erişim sadece Ukrayna değil, tüm Orta ve Doğu Avrupa'da kesintiye uğramış, ama uydunun sahibi olan Amerikan Viasat firmasının saatler içerisinde geliştirip devreye soktuğu yazılım güncellemesi sayesinde siber müdahale etkisiz kılınarak erişim [tekrar sağlanmıştır](#). Savaşın sadece öncesi ve ilk evresinde değil, takip eden evrelerinde de Rusya'nın siber saldırılarının hız kesmeden devam ettiği anlaşılmaktadır. Sadece mart ayı içerisinde tespit edilen siber saldırı sayısı [120'nin üzerindedir](#). Ama yine de Rus siber saldırılarından önemli ve kalıcı sonuç alınamaması durumu bugüne kadar devam etmiştir.

Rusya-Ukrayna Savaşı'nda siber savaş bağlamında altının önemle çizilmesi gereken bir diğer önemli gelişme, 2014 yılındaki gelişmelerden farklı olarak, Ukrayna'nın çaresiz kalmak bir yana, Rusya'ya karşı etkin siber saldırı ve engelleme faaliyeti içerisine girmesi ve günler içerisinde Rusya'yı siber ortamdaki mücadelenin zararlı çıkarı konumuna düşürmesidir. Ukrayna'nın devasa boyutlara ulaşan siber savunma ve saldırı faaliyetleri, silahlı kuvvetleri bünyesindeki uzman personel ve Ukrayna'nın görece gelişmiş bilişim sektörünün yanı sıra, Dünya'nın dört bir yanından Ukrayna'ya destek veren gönüllü internet korsanlarınca [yürütülmektedir](#). Ukraynalı yetkililer bu gönüllüler ordusuna belli zaman dilimlerinde belli hedefler göstermekte, devamında gerçekleşen ve kitlesel hedef alma (*crowd targeting*) sonucunda, Rusya'nın ağırlıklı olarak resmî kurumlarınca yürütülen internete dayalı faaliyetleri akamete uğratılmakta, ayrıca Rus devlet kurumları ve şirketlerine ait her türlü veri ele geçirilerek internet üzerinden paylaşımına açılmaktadır. Moskova'nın kendi siber saldırılarına ayırabildiği kaynakları da ciddi olarak sınırlayan bu saldırılar karşısında, Rusya yurtdışıyla internet trafiğini kısıtlamak [zorunda kalmıştır](#).

Rusya'ya karşı yürütülen siber saldırılar, sadece Ukrayna tarafından veya gönüllü korsanlarca yürütülmemekte, NATO, ABD ve Ukrayna'ya destek veren diğer devletlerin de ellerindeki siber saldırı imkanlarını Ukrayna'nın yanında Rusya'ya karşı devreye soktukları düşünülmektedir. NATO, savaşın başlamasından önceki aylarda bazı Doğu Avrupa ülkelerine siber timler konuşlandırmış olmasının ötesinde, siber alanda Ukrayna'ya verdiği destekle ilgili son derece temkinli bir söylem benimseyerek kamuoyuyla [bilgi paylaşmaktan kaçınmaktadır](#). Buna karşılık ABD'li yetkililer, daha önce hiç yapmadıkları bir şeyi yaparak, ABD Siber Komutanlığı personelinin Aralık 2021'de Ukrayna'da göreve başladığını ve ABD'nin Rusya'ya yönelik siber harp faaliyetlerinin sadece savunma değil, saldırı boyutunu da içerdiğini [resmen açıklamışlardır](#). Başka bir deyişle, Rusya karşısındaki siber mücadelenin, Ukrayna'nın tek başına yürüttüğü bir mücadele olarak değil, en azından ABD ve diğer bazı NATO üyelerinin iş birliğiyle yürütülen bir mücadele olarak görülmesi gerekir. Varılan bu sonuç, Rus siber saldırılarının uğradığı başarısızlığı ve Rusya'nın siber saldırıların kurbanı haline gelmiş olmasını açıklıyor olabilir. Eklenmesi gereken bir diğer önemli not, Rusya'nın siber saldırılarının sadece Ukrayna'yı hedef almadığı, başta ABD, Polonya, Baltık ülkeleri,

İsveç ve Finlandiya olmak üzere toplam 42 ülkedeki hedeflere yönelik yüzlerce Rus siber saldırısının [tespit edilmiş olmasıdır](#).

Sonuç itibarıyla, Rusya-Ukrayna Savaşı sayesinde siber saldırıların savaşın fiziki boyuttaki seyirini ve sonucunu belirleyecek veya bazılarınca iddia edildiği üzere oyunun kurallarını kökten değiştirecek askeri bir yetenek türü olmadığı anlaşılmıştır. Özellikle tarafların siber saldırılar karşısında belli bir hazırlık seviyesinde olduğu askeri çatışma senaryolarında, hedefler üzerinde fiziki hasar yaratan bombaların ve füzelerin siber silahlardan çok daha kullanışlı ve etkisi kesin savaş araçları olduğu bu vesileyle [teyit edilmiştir](#).

Karşı Uzay

İngilizcedeki ‘*counter-space*’ terimine karşılık olarak kullanılan ‘karşı uzay’ kavramı, Dünya’nın yörüngesindeki uydulara zarar vermeye, bunların hizmetlerini geçici veya kalıcı olarak aksatmaya yönelik girişimleri içermektedir. Bu kapsamda, salt uydulara yapılan taciz, engelleme ve saldırılar değil, bu uyduların bağımlı olduğu yerküre üzerindeki altyapı unsurlarına yönelik müdahaleler ve ilaveten uydular üzerinden sağlanan haberleşme, keşif, takip ve gözetleme ve konum tespiti gibi çok geniş bir yelpazeye yayılmış hizmetlerin engellenmesine yönelik girişimler de karşı uzay çerçevesinde değerlendirilmelidir.

Uydulara yönelik girişimler dendiğinde ilk akla gelen uydusavar silahlara (*anti-satellite – ASAT*), yani yeryüzünden yörüngedeki uydulara doğru fırlatılan füzelere ABD, Çin ve Hindistan’ın yanı sıra Rusya Federasyonu da sahiptir. Hatta Rusya bunlardan birisini Kasım 2021’de yörüngedeki kullanım dışı bir uydusunu vurarak [denemiştir](#). Ayrıca, yörüngeye yerleştirilecek uzay araçlarıyla uydulara zarar verilmesi veya uyduların hizmetlerinin kesintiye uğratılması mümkün olup, Rusya bu yetenekte uzay araçlarına da [sahiptir](#). Buna karşılık, Rusya-Ukrayna Savaşı sırasında Moskova, uzaydaki uyduları doğrudan hedef almaktan kaçınmış, yerine bu uydulardan Ukrayna’ya gönderilen sinyalleri bastırmaya çalışmış ya da uyduların karasal altyapı ve/veya terminallerine yönelik siber ve elektronik harp saldırılarında bulunmuştur. Başka ülkelerin uydularına yönelik bu türden taciz ve engellemelere daha önce rastlandığı halde, Rusya’nın Ukrayna’ya yönelik saldırıları, iki devlet arasındaki bir savaşta uzay üzerinden sağlanan hizmetlere yönelik harp tarihindeki ilk örnekleri teşkil etmektedir.

Açık kaynaklara yansıdığı kadarıyla, en az üç Rus karşı uzay girişimi gerçekleşmiştir. Bunlardan ilkinde daha önce siber saldırılar alt başlığı altında değinilmiş olup, Doğu Avrupa’ya hizmet veren KA-ASAT haberleşme uydusunun karasal altyapısı ve uzantıları, Rus ordusunun Ukrayna’ya girmesinden birkaç saat önce siber müdahaleyle hizmet dışı bırakılmıştır. Ukrayna’nın yanı sıra Doğu ve Orta Avrupa’daki kullanıcıları da uydu erişiminden mahrum bırakan bu saldırı, uyduyu işleten ABD Viasat firmasının farklı bir yazılım sürümünü devreye sokmasıyla kısa sürede [etkisiz kılınmıştır](#). İkinci saldırı da ilkiyle neredeyse aynı zaman diliminde gerçekleşmiş ve SpaceX firmasının savaşın başlamasından önce Ukrayna ordusuna hibe edilen Starlink uydu haberleşme mobil terminalleri, bazı kaynaklara göre siber saldırı yoluyla, diğer kaynaklara göre elektronik harp teknikleriyle, yani RF sinyalleri gönderilerek karıştırılmıştır. Bahse konu saldırı da SpaceX firmasının büyük olasılıkla yazılım temelli önlemleri sayesinde [savuşturulmuştur](#).

Üçüncü kategori saldırıdaysa, uzaydaki ABD uydularından gönderilen ve konum tespiti ile seyrüsefer ve hedef tayininde kullanılan Küresel Konumlama Sistemi (GPS) sinyalleri, Rusya tarafından Ukrayna’nın belli bölgelerine daha güçlü veya kirletilmiş sinyaller gönderilmesi suretiyle karıştırılmıştır. Rusya, 2014’ten beri Karadeniz ve Baltık bölgelerindeki NATO tatbikatları sırasında benzer karıştırma tekniklerine başvurmakta ve komşu ülkelerin protestoları ile karşılaşmaktaydı. Dolayısıyla, GPS sinyallerine yönelik bastırma ve kirletme girişiminin Ukrayna’da kullanılması sürpriz olmamıştır. Buna karşılık, Rusya’nın uzaydan

gelen GPS sinyallerini bastırma konusunda sahip olduğuna inanılan ileri kabiliyetlerin, Rusya-Ukrayna Savaşı'nın seyri üzerinde fazlaca bir etki yaratmamış olması birçok gözlemci tarafından ilginç bulunmuştur. Getirilen açıklamalar arasında öne çıkan, GPS'in Rus muadili *Glonass* sistemine ait yeterli miktarda terminale sahip bulunmayan Rus silahlı kuvvetlerinin de GPS sinyallerinden istifade ediyor olması sebebiyle, GPS'e yönelik karıştırmanın asgari seviyede tutulduğu [iddiasıdır](#). Getirilen diğer bir açıklama ise, Rusya'nın diğer pek çok alanda olduğu gibi bu konudaki teknolojik kapasitesinin de beklendiği kadar ileri olmadığı veya karıştırma sistemlerinin yerinin süratle tespit edilip vurulmasından çekindiği için bunları [aktif hale getirmediğidir](#).

Rusya-Ukrayna Savaşı sırasında sahada gözlenen ve etkinliği tartışmalı karşı uzay girişimleriyle ilgili yapılabilecek diğer bir gözlem de, ABD ile Rusya'nın bu tür karşı uzay saldırılarına verecekleri yanıtın ne olacağına dair caydırıcılık söylemlerinde meydana gelen değişiklik ve kaymalardır. ABD'nin Soğuk Savaş yıllarından bu yana benimsemiş olduğu ve daha yakın zamanda Trump Yönetimi'nce teyit edilen caydırıcılık söyleminde, uydulara karşı nükleer olmayan silahlarla gerçekleştirilecek ve ABD'nin nükleer komuta-kontrol-haberleşme kapasitesini tehlikeye sokacak saldırılara, ABD'nin nükleer silah kullanarak karşılık vereceği [uyarısında bulunmaktadır](#). Halbuki Rusya-Ukrayna savaşının başlamasından birkaç hafta sonra Amerikalı yetkililer, konum tespit ya da haberleşme sinyallerinin karıştırılması gibi kalıcı etkisi bulunmayan uydulara yönelik müdahaleleri kabul edilebilir ve 'rutin savaş faaliyetleri' olarak gördüklerini açıklayarak, uyduların kendisi değil ama sağladıkları hizmetlere yönelik saldırıları bir bakıma [normalleştirmişlerdir](#).

Savaşın başlamasından sonra bunun tam aksi yönde bir pozisyona kayan Rus yetkililer ise, daha önceki yıllarda belirsiz olan uzaya yönelik caydırıcılık pozisyonlarını sertleştirerek, uzaydaki uydulara erişimi engellemeye yönelik girişimlerin Rusya tarafından *casus belli*, yani savaş sebebi sayılacağını [ilan etmişlerdir](#). Başka bir ifadeyle Rusya, Ukrayna'nın kullandığı ABD mülkiyetindeki uydulara karşı kendisinin gerçekleştirdiği saldırıların benzerlerinin Rus uydularına yapılmasını savaş sebebi sayılacağını ilan ederek, kendi içerisinde tutarsız ve savunulması zor bir caydırıcılık düzlemine kaymıştır. Bu tepkinin altında, normalde askeri nitelikli saldırılar karşısındaki direncinin düşük olması beklenebilecek Batılı ülkelere ait ticari uyduların bile, Rusya'nın saldırılarını ne denli kolaylıkla savuşturabildiklerinin görülmüş olmasından kaynaklanan zafiyet algısı ve kendine güvenin sarsılması olabilir. Nitekim Rusya'nın uzay faaliyetlerinin başındaki yetkilinin, dünya genelinde uzayla uğraşan devlet ve özel sektör oyuncularının tamamının artık sadece Rusya'nın düşmanları hesabına çalıştığını ifade etmiş olması, Rus siyaset yapımcıların bu konuda duydukları öfke, yalnızlık ve kaygıların yansması olarak [yorumlanabilir](#). Sonuç olarak, Rusya-Ukrayna Savaşı'nın karşı uzay boyutunun da daha önce incelenen diğer iki YBT'ye benzer şekilde, Rusya açısından hiç de olumlu gözlemler ve dersler içermediği söylenebilir.

Sonuç ve dersler

Uluslararası güvenlik ile bilim ve teknoloji çalışan araştırmacıların neredeyse tamamınca YBT niteliği taşıdığı kabul edilen hipersonik silahlar, siber saldırılar ve karşı uzay, Rusya-Ukrayna Savaşı vesilesiyle konvansiyonel bir çatışmada ilk kez sahne almıştır. Bu yönüyle, en azından bahse konu üç YBT açısından gelecekteki savaşların kaçınılmaz parçası olacağı yönündeki öngörü doğru çıkmıştır.

Buna karşılık, birçok araştırmacı tarafından teknolojik imkanları görece ileri devletler arasındaki ilk büyük çaplı savaşta sahaya sürüleceği kehanetinde bulunulan diğer bazı YBT'lerin, örneğin yapay zekâ destekli otonom silahların kullanımına tanık olunmamıştır. İlâveten, hem yaygın ve şiddetli siber saldırıların, hem de uzaydaki uydulara yönelik saldırı ve

engellemelerin, hedefteki devletin savařma kapasitesini sekteye uęratacaęı, hatta o ¼lkedeki g¼nl¼k yařamı felce uęratabileceęi uyarılarının da abartılı olduęu anlařılmıřtır. Fakat bu ıkarımın gerek karřı uzay gerekse siber saldırılar karřısında asgari tedbirlerini almıř ve belli bir teknolojik potansiyeli haiz devletler iin geerli olduęu, buna karřılık 2014 yılında Kırım'ın iřgalinde g¼r¼ld¼ę¼ ¼zere, taraflardan en az birisinin yeterince hazırlıklı olmadıęı atıřma senaryolarında, karřı uzay ve siber saldırıların olumsuz etkilerinin ok daha derin olabileceęinin altı izilmelidir.

Hem karřı uzay hem siber saldırılar baęlamında dikkat ekilmesi gereken bir dięer husus, bu iki mecrada gerekleřen saldırıların sadece hedefteki devletleri deęil, savařa taraf olmayan bařka ¼lkelerdeki sivil, askeri veya kritik altyapı kullanıcılarını da olumsuz y¼nde etkiledięidir. Dolayısıyla, bu iki YBT'nin en azından bug¼ne kadar kullanılagelmiř konvansiyonel harp silah ve vasıtalarına kıyasla, devlet sınırlarını kolaylıkla ařma potansiyeli ve tehlikesinin daha y¼ksek olduęu, dolayısıyla uluslararası g¼venlik iin bu y¼n¼yle de risk teřkil ettikleri vurgulanmalıdır.

Rusya-Ukrayna Savařı, hipersonik silahların bir savařta ilk kez kullanımına sahne olduęu halde, aslında hipersonik silahlara bařvurulmasını gerektirecek řartlar mevcut olmadıęından, bu kullanımın savařın seyri ¼zerinde herhangi bir etkisi olmamıř, tırmandırıcı veya istikrarı bozucu bir sonu da ortaya ıkmamıřtır. Dięer taraftan, ¼zellikle f¼ze savunma kabiliyetine ve/veya n¼kleer harp bařlıklarına sahip hasımlar arasındaki kriz ve atıřma senaryolarında, hipersonik silahların istikrarsızlařtırıcı ve tırmandırıcı etkilerine hala dikkat edilmesi gerekecektir. Ayrıca, hipersonik silahların bundan b¼yle balistik f¼zeler ve seyir f¼zelerinin yanı sıra gelecekteki savařların olaęan harp vasıta ve silahları arasında yer alması beklenmelidir. Bařat g¼lere ilaveten, d¼nyanın ¼nde gelen birok b¼lgesel g¼c¼n¼n de hipersonik silahları envanterlerine dahil etmekte olmaları da bu beklentiye desteklemektedir.